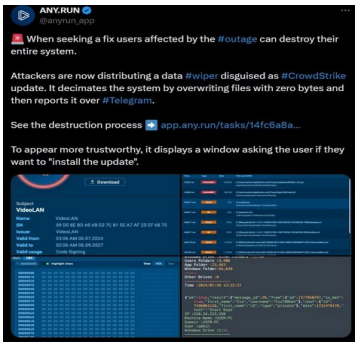
The following was posted on a channel named “Pro-Palestine Hackers Movement (PPHM)”.

“Stay tuned for up-to-date cyber news with a pro-Palestine approach.
Contact for Cooperation and News: @pphm_admin
Instagram: https://www.instagram.com/pphm_news
Twitter: https://twitter.com/PPHM_1”

Sunday, July 21, 2024


ANY.RUN
@anyrun_app
When seeking a fix users affected by the #outage can destroy their entire system.
Attackers are now distributing a data #wiper disguised as #CrowdStrike update. It decimates the system by overwriting files with zero bytes and then reports it over #Telegram.
See the destruction process app.any.run/tasks/14fc6a8a...
To appear more trustworthy, it displays a window asking the user if they want to “install the update”.

“Handala targeted thousands of Israeli organizations!
Several organizations of Israel have lost terabytes of their data so far.
INCD is also confused!”

Monday, July 22, 2024

brain cipher
Main
FAQ
Rules
FAMILY
Wealth Advisors
Family Wealth Advisors Ltd.
Family Wealth Advisors is an independent boutique family office which provides a broad set of services to a High-Net-worth Individuals and families.
Download available in:

“The Israeli company, FWA, has been hacked by Brain Cipher group.”

July 31, 2024

“The Canadian company, Bausch Health is faced a ransomware attack. They are supposed to pay 3 million dollars for the safety of their information.”

Challenge Group

30.07.2024

Dear Customers and suppliers,

We wish to inform you that our group is currently experiencing data disruptions, which may be due to a cyber-attack. The result is that some of our group servers are down, affecting our operations.

The IT team is working tirelessly to resolve the situation and is in the process of restoring systems from our backups. Prioritizing critical services is our top priority, and we will keep you updated on our progress.

Please be assured that we are taking all necessary measures to resolve this issue as quickly as possible. We will provide further updates as more information becomes available.

Thank you for your understanding and cooperation.

Or Zak – Challenge Group CCO

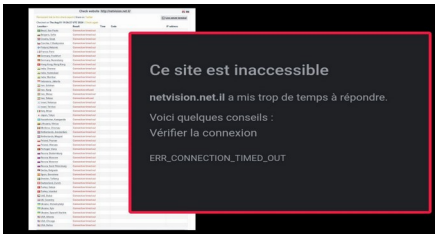
“Challenge Airlines, an Israeli cargo transportation company, is under a ransomware attack!”

August 1, 2024

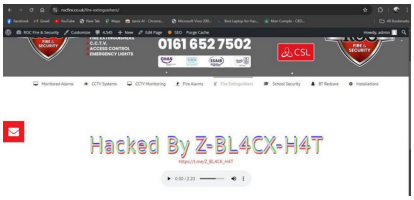
“Hunt3r kill3rs penetrated into Rafael servers and got access to information of all its employees!”

August 2, 2024

DATABASE 3.9 Million Israel Citizens DB
THIS DATA WAS OBTAINED BY VIRUSEC OVER 3.9 MILLION LINES AND IS ALWAYS FIRSTHAND!!
phone | uid | email | first_name | last_name | gender | date_registered | birthday | location | hometown | relationship_status | education_last_year | work_groups | pages | last_update
lines: 3.9 million
TO UNLOCK PLEASE REPLY TO THIS THREAD!!
Hidden Content
Shop: @ViruSec
“3.9 million DB of Israeli citizens has been leaked by virusec.”


Ce site est inaccessible
netvision.net.il a mis trop de temps à répondre.
Voici quelques conseils :
Vérifier la connexion
ERR_CONNECTION_TIMED_OUT
“Moroccan Black Cyber Army took down the largest services and communications provider in Israel!
http://netvision.net.il/
https://check-host.net/check-report/1caca38fk727”

August 3, 2024



“Z_BL4CX_H4T hacked rocfire.co.uk/fire-extinguishers/”

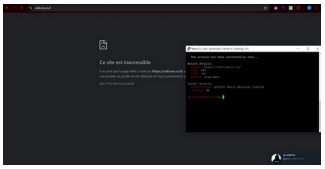
MOROCCAN DRAGONS
CYBER TEAM
- PWNED BY MOROCCAN DRAGONS -
- WE WILL NOT STOP ATTACKING ISRAEL -
- FREE PALESTINE & FUCK ISRAEL -
ABOUT US
TELEGRAM
© 2024 ALL RIGHTS RESZRVED
“Moroccan Dragons attacked an American website!
https://shauntfitness.com/”

August 5, 2024

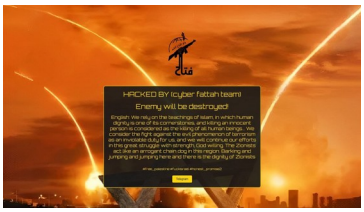
“Israel Badz Beit Yosef is under ransomware attack!
They are going get 250,000 dollars in return for the sensitive data.”

“CyberVolk attacked an Israeli website!
http://moss.tel-aviv.gov.il/
https://check-host.net/check-report/1ccff266k6df”

Tuesday, August 6, 2024


“NetForceZ took down cellcom.co.il.”

Wednesday, August 7, 2024



“Web servers that contain British commercial and also some industrial websites have been hacked by Cyber Fattah Team!

aiisar.com
bestbuyingshop.com

digitalmarketingsol.uk
enlivenlogistics.com
enliventechnologies.co
enlivenwebsolutions.com
hsmercantile.ltd
mybestbuyingshop.com
samz-wholesale.co.uk
saudiataxibooking.com
tarpaulinssheets.co.uk
tarpaulinswholesale.co.uk
thetarpaulinssheet.co.uk
xm-squared.com

✔check:
https://www.zone-h.org/archive/notifier=Hmei7”

Sunday, August 11, 2024

“Tyrek company in Israel has been target of a cyberattack!
Tyrek is a leading company in the collection and recycling of tires.”

“Doubleface defaced some Israeli websites!

https://bluesunrisedubai.com
http://dyb.co.il
https://eliteaestheticss.com
https://ha-gina.com
https://hotties.co.il
https://indexstyle.co.il
https://metro-jerusalem.co.il
https://mirk.co.il
https://rafi-varditmusic.com
https://shuli.org.il
https://veata-kadosh.com/”

Wednesday, August 14, 2024

“The Swiss company Schlatter Group is under a ransomware attack! All computers and emails are disrupted.”

“NoName057 with help of Holy League and 7 October Union attacked Israeli websites!

NoName057

http://check-host.net/check-report/1d1e3019kdb

http://check-host.net/check-report/1d1e33aaka74

http://check-host.net/check-report/1d1e3649kf55

http://check-host.net/check-report/1d1e3e12k286

http://check-host.net/check-report/1d1e42a6k593

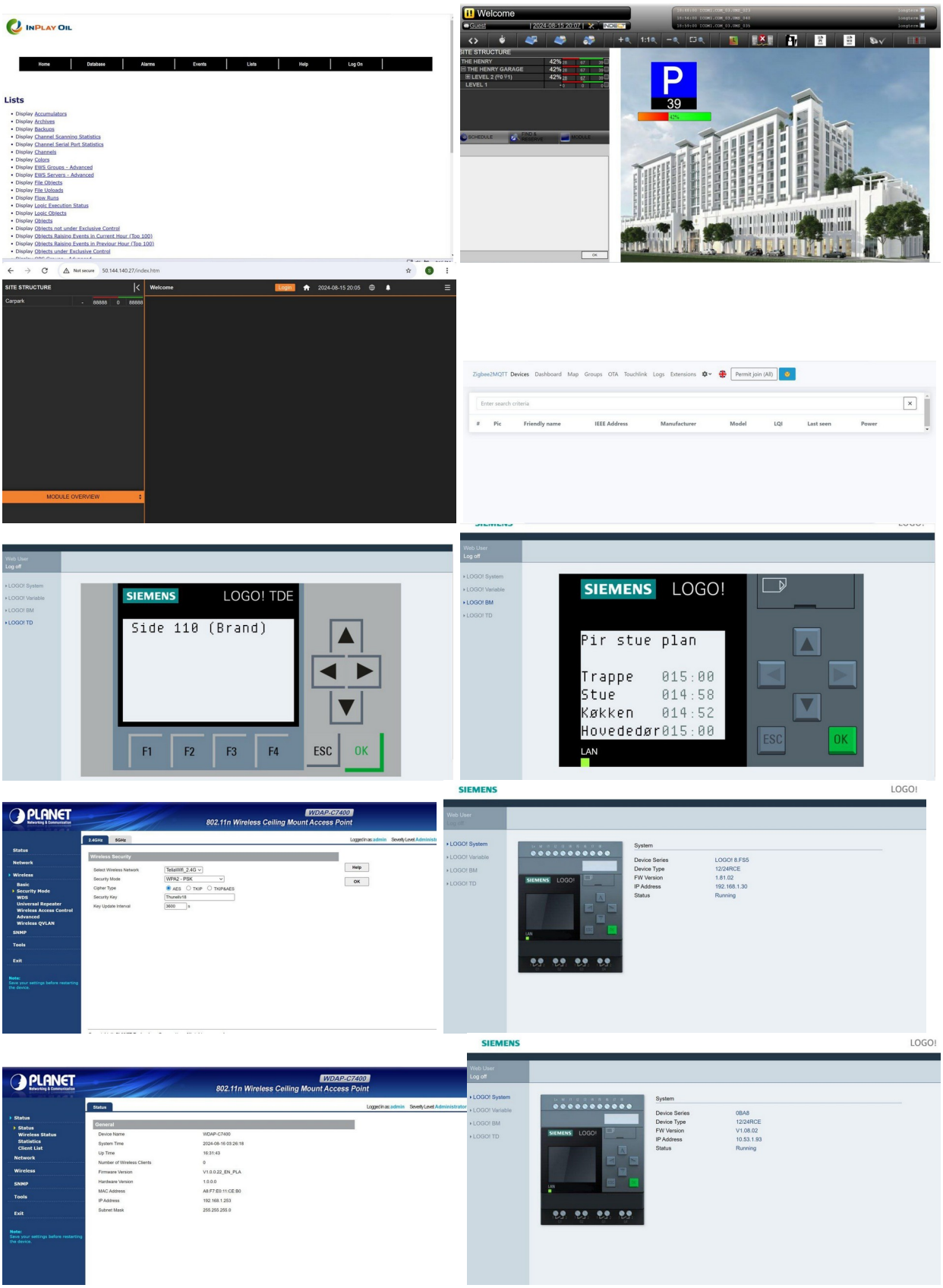
http://check-host.net/check-report/1d1e43e5ke13

http://check-host.net/check-report/1d1e474ak4fc

http://check-host.net/check-report/1d1e49eckc22

http://check-host.net/check-report/1d1e4ceek300”

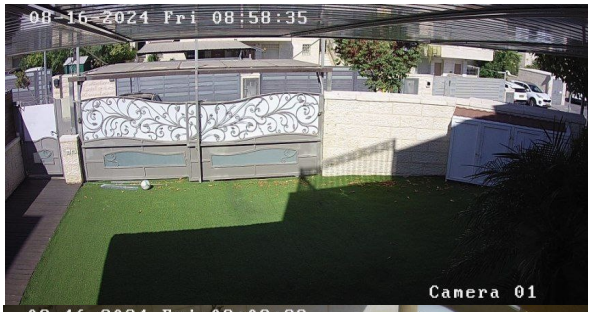
Saturday, August 17, 2024

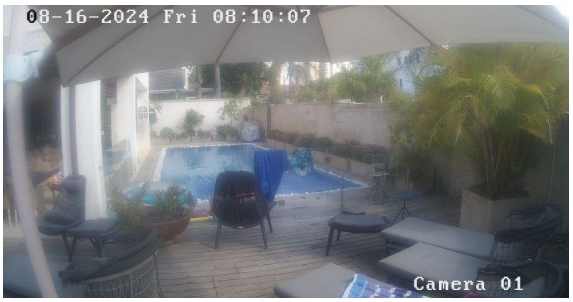


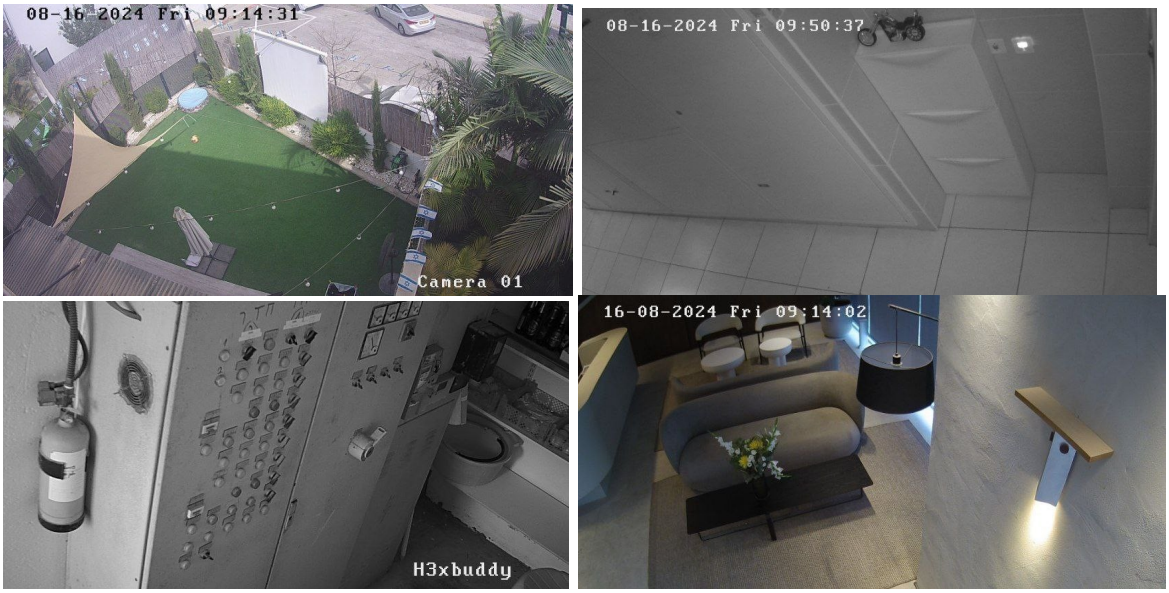
“Hunt3r kill3rs attacked infrastructures of America and NATO countries!”

“Union, the Crypto company is exposed to a cyberattack!
Attacker succeed to get to company's Google G-Suite management interface and change passwords.”

HACKED BY DIMAX66
Stupid Israel Fuck You Guys
"Relying on a single layer of security is like locking your front door but leaving the window wide open."
In the holy land of Palestine, there will be a day when the flag of Palestine independence will fly majestically
Your System Low Security
“DIMAX66 hacked an Israeli website!”



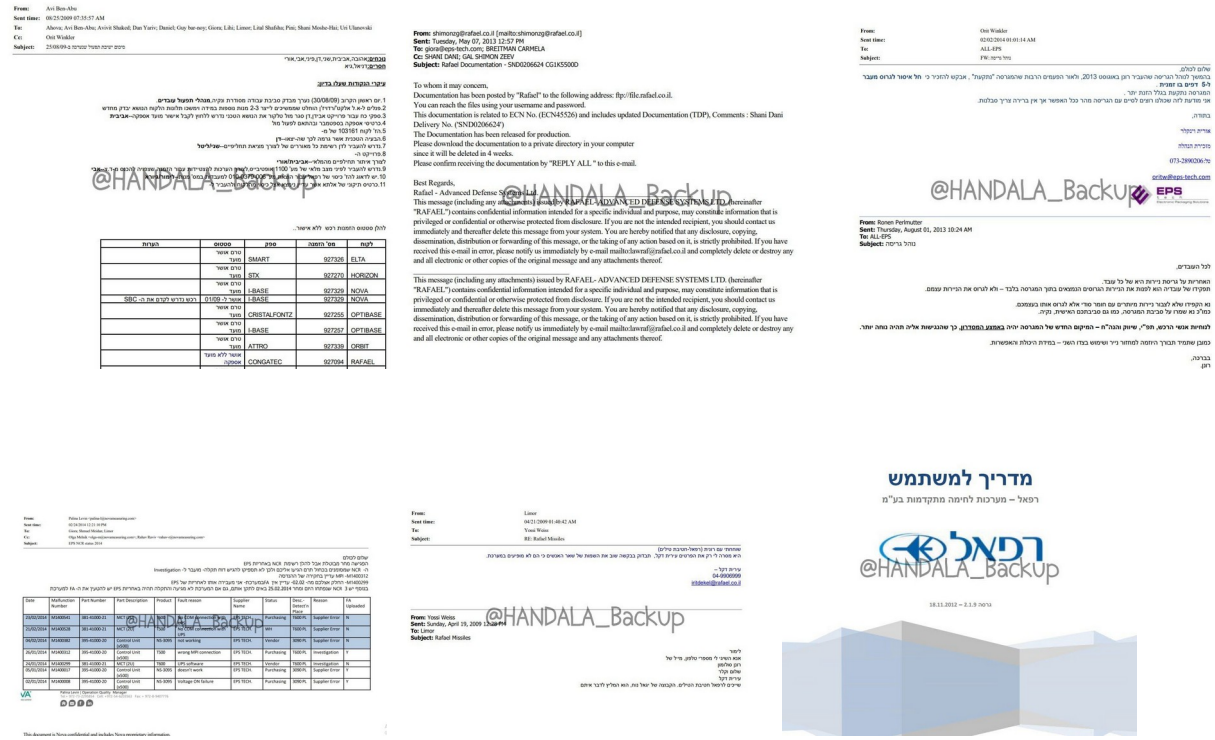




“Moroccan Dragons hacked 20 Israeli cameras!
93.173.94.42
149.106.149.176
79.178.30.181
212.143.177.222
85.130.140.207
149.106.243.172
5.29.102.121
213.57.144.27
149.106.236.134
85.130.235.22
85.130.216.77
79.180.67.250
213.57.235.4
85.130.239.119
85.130.239.123
85.130.212.133
109.226.49.66
85.130.161.163
213.8.125.108”

Monday, August 19, 2024

“Hunt3r kill3rs hacked Rafael company and got access to their documents!”



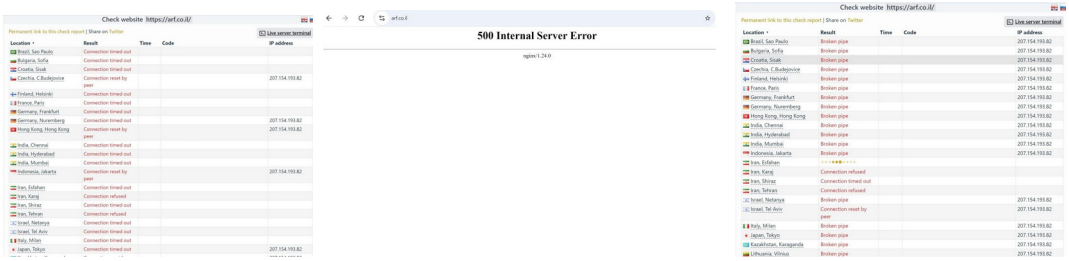
“Handala revealed over 150K emails of EPS Tech!”

“Gan Shmuel Company, the Israeli company that produces raw materials for soft drinks industry, is exposed to information leak!”

- PWNED BY MOROCCAN DRAGONS -
- WE WILL NOT STOP ATTACKING ISRAEL -
- FREE PALESTINE & FUCK ISRAEL -
ABOUT US TELEGRAM
© 2024 ALL RIGHTS RESZRVED

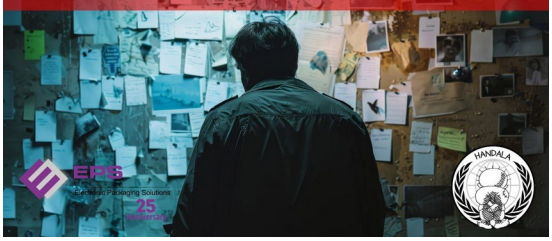
“Moroccan Dragons took down the American website ptr-transport.com”

Saturday, August 24, 2024



“Ashdod Refinery company faced a cyberattack by Hunt3r kill3rs!”

Employee List of EPS Tech



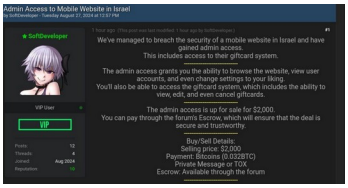
נטליה אמטוב	natalja1462@gmail.com	972547238675
יצחק שגיא	Yitzhak@eps-tech.com	972544339393
דימה רבץ	dimar@eps-tech.com	972545933596
גנדי פורמנוב	Gennadyf@eps-tech.com	972526097355
לימור כהן גזז	Limor@eps-tech.com	972523584222
אברהם נתן בחכמה	avrahamn.b@eps-tech.com	972587190773
אבי וילנסקי	aviwilenski@gmail.com	972507104180
אלה ליבשיץ	Ella@eps-tech.com	972547672900
גיורא גלסמן	Giora@eps-tech.com	972523588320
גרגורי צ'רקס	Gregoric@eps-tech.com	972526862309
יבגני אמינוב	Yevgeni@eps-tech.com	972507957875
קיריל פינסקי	kiril.p@eps-tech.com	972545332300
ולרי פסחוב	Valeryp@eps-tech.com	972544796817
אבי בן אבו	Avi@eps-tech.com	972523588319
פיני עזריה	Pini@eps-tech.com	972523412335
גלב רוטשטיין	grxhch@gmail.com	972548022275
אביתר שמחי	evyatar.s@eps-tech.com	972502822665
איתן פרזס	eitan@eps-tech.com	972548461648
יוסי וייס	Yossiw@eps-tech.com	972523555138
כפאייה שייך יוסף	kefaia.sh29@gmail.com	972507839430
סרגיי צ'רקסקי	viki28@zahav.net.il	972523856338
איתן תהילה	Eitant@eps-tech.com	972523904185
דוד חורם-יאן	david.k@eps-tech.com	972545250820
יעקב גז'ס	yakov.g@eps-tech.com	972507752301
אייל בלך	Eyal.b@eps-tech.com	972524008136
שמעון אבן חיים	shimon.e@eps-tech.com	972547841045
נפתלי דהן	NaftaliD@eps-tech.com	972524696014
שרון שפירא	sharon.s@eps-tech.com	972545620582
אילן ברנד	IlanB@eps-tech.com	972528477526
עודד אמיר	oded.a@eps-tech.com	972547771759
עופרי אפלבאום	ofriapple2712@gmail.com	972523457487
גיא בר נוי	Guy.B@eps-tech.com	972523904183
רוברט שטוטמן	robert.shtutman@gmail.com	972545855568
אלכס גלטר	alex@eps-tech.com	972549438665
נסים איקסלין	nisimek@walla.com	972536215716
שמעון וינריך	Shimon@eps-tech.com	972546577863
שרית עצמון יוסף	Sarit@eps-tech.com	972506364264
מיכאל ציפין	Michael@eps-tech.com	972523735234
איגור אהרונוב	Igor@eps-tech.com	972544808553
הראל אדרעי	harel.e@eps-tech.com	972545438978
רחל מישקין	rachel.m@eps-tech.com	972506480159
אולג איגנויאן	oleg@eps-tech.com	972524330964
הרצל שיריאן	herzel.s@eps-tech.com	972523589857
דניאל אפלבאום	Daniel@eps-tech.com	972523588315
סמיון יחאוסקין	SemionY@eps-tech.com	972523588318
תמר אלפואר	Tamar@eps-tech.com	972504437170
מיכאל שחנובצקי	michael.s@eps-tech.com	972526822032

“Information of some employees of EPS Tech has been leaked by Handala!”
Monday, August 26, 2024

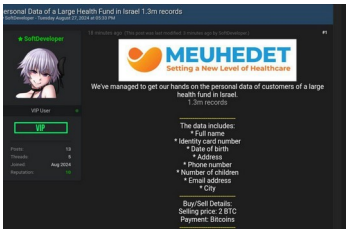
11:21 AM

“Seattle Airport is out of service due to a cyberattack!
Different services such as emails, telephones, websites, etc. are down.”

Wednesday, August 28, 2024


Admin Access to Mobile Website in Israel
SoftDeveloper
VIP User
VIP
We've managed to breach the security of a mobile website in Israel and have gained admin access.
This includes access to their giftcard system.
The admin access grants you the ability to browse the website, view user accounts, and even change settings to your liking.
You'll also be able to access the giftcard system, which includes the ability to view, edit, and even cancel giftcards.
The admin access is up for sale for $2,000.
You can pay through the forum's Escrow, which will ensure that the deal is secure and trustworthy.
Buy/Sell Details:
Selling price: $2,000
Payment: Bitcoins (0.032BTC)
Private Message or TOX
Escrow: Available through the forum

“Access to a mobile website in Israel is going to be sold out!”



“The same attacker also offers for sale information of a health fund in Israel!”
Thursday, August 29, 2024

Exclusive Access to Large Israel IT Company Cloud Infrastructure
SoftDeveloper
VIP User
VIP
We are pleased to offer an opportunity to acquire access to the cloud infrastructure of Large Israel IT Company.
What's Included:
Comprehensive access to the company VPN network
Full RDP (Remote Desktop Protocol)
12TB of data
The access is up for sale for $150,000
Buy/Sell Details:
Selling price: $150,000
Payment: Bitcoins

“SoftDeveloper this time sells full access to the cloud entertainment of a large IT company in Israel for $150k!”

“Hunt3r kill3rs sells database of Israel military and intelligence services!”

Thursday, September 5, 2024

“These Israeli websites have been under cyberattack these days:

هذه المواقع الإسرائيلية تعرضت لهجوم إلكتروني هذه الأيام:

leumi.co.il
aisrael.org
science.co.il
winnerscode.co.il
oneforisrael.org
danyel.co.il
school.iasa.org.il
e-kitchens.co.il
bneiakiva.org.il
netstep.co.il
yadezra.net
nsogroup.com
ybz.org.il
boi.org.il
z-school.co.il
treehouse.co.il
nativ.centaur.co.il”

“Planned Parenthood Medical Center in New York is exposed to a ransomware attack!”

Saturday, September 7, 2024

“*25 American websites are vulnerable!*
EthersecTeamCyber hacked 25 websites of America and they are out of service!

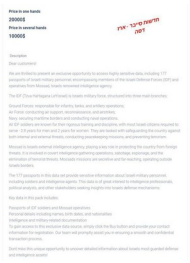
https://acictofficial.com/ETC.html
https://avivakeeon.com/ETC.html
https://avivakeeoninterio.com/ETC.html
https://cadetsacademy.com/ETC.html
https://cadetsacademy.in/ETC.html
http://cadetsacademy.org/ETC.html
https://cistbijnor.com/ETC.html

http://cleantree.co.in/ETC.html
https://colour-tribe.com/ETC.html
https://dnsmachines.com/ETC.html
https://envirowrap.co.in/ETC.html
https://eros-group.co/ETC.html
https://freedomhomes.in/ETC.html
https://goldengrande.biz/ETC.html
https://jobmilgai.com/ETC.html
https://manchias.com/ETC.html
https://manchias.in/ETC.html
https://noidaexpresswayfarmhouse.com/ETC.html
https://novovitahealthcare.com/ETC.html
http://shrimadshauryaacademy.in/ETC.html
https://scginfo.com/ETC.html
https://shrimadshaurya.in/ETC.html
https://thegoldenstariconawards.com/ETC.html”

Sunday, September 8, 2024

“AVIS, the American car rental company, is under a cyberattack!”

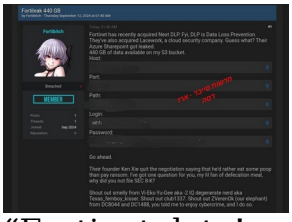
Wednesday, September 11, 2024



“Information of Mossad and Israeli military agents are for sale for $20k!”

Saturday, September 14, 2024

“London-City Airport has been shut down. The web resource is currently unavailable.
All day long, together with NoName057(16) & CyberArmy, we work on Great Britain. While requests fill the English servers, we try to penetrate their infrastructure.”



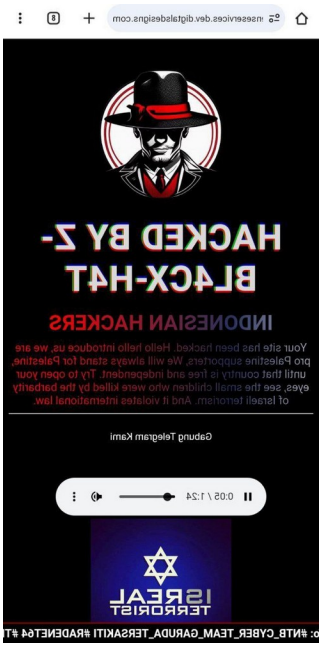
“Fortinet data!
440GB of Fortinet information has been stolen!
Information was obtained from the SharePoint of companies purchased by Fortinet.”

“Digital Lobby, which provides remote control screens, is under a massive cyberattack!”

Sunday, September 15, 2024

“Security Information of several organizations in Israel is for sale!
The attack occurred by a malware.”

Monday, September 16, 2024



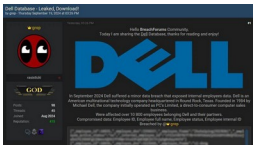
“ADS, the only defense article provider in the U.S has been target of Z_BL4CX_H4T!

https://alieddefenseservices.dev.digtalsdesigns.com/”

Tuesday, September 17, 2024

“Johnson School District in the state of Tennessee, USA faced a cyberattack through an email scam!”

Sunday, September 22, 2024



“DELL & a massive cyberattack!
DELL company is under a cyberattack and information of 10,800 of their employees has been stolen.”

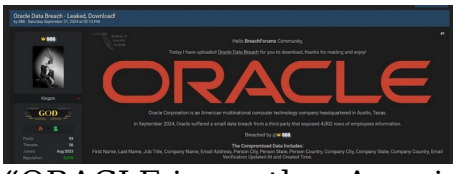
“Heavy attacks of NoName057 on Israel internet infrastructure!

Municipal information of Israel (closed by geo)
check-host.net/check-report/1e892606k7dc

Delek Group is an Israeli holding conglomerate operating mainly in the oil industry
check-host.net/check-report/1e8927a7k5d4

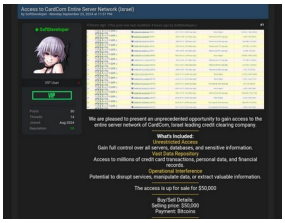
Authorization on the portal of the Odix edge server
check-host.net/check-report/1e8929eak703”
Monday, September 23, 2024

“Data of 1 million users of American Banking Credit Loan is leaked!”



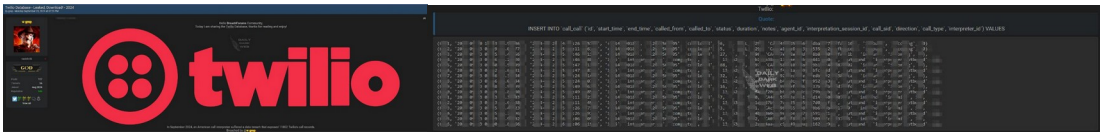
“ORACLE is another American company that is under a data breach!
4k sensitive employees details leaked.”

Tuesday, September 24, 2024

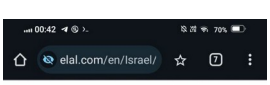


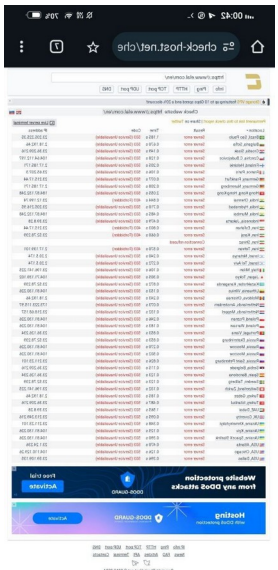
“The Israeli company Cardcom!
Access to network of the clearing company, Cardom is for sale for $50k.”

“MoneyGram, money transfer company, has been hacked!”



“Twilio, the American company working in the field of communications, exposed to data breach!”





“AlAhad hacked Israel Airlines!
https://check-host.net/check-report/1e990416kc6e”

Thursday, September 26, 2024

“UK police under cyberattack!
The British police announced that 19 train stations have been target of cyberattack.”

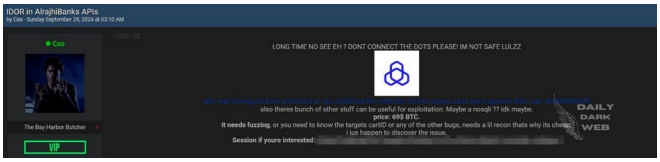
Saturday, September 28, 2024

“The Israeli company PipelBiz is the new victim of Ransomhub!”

“A hacking group attacked Natalie Medical Services of Israel and stole 100GB from the company's network!”

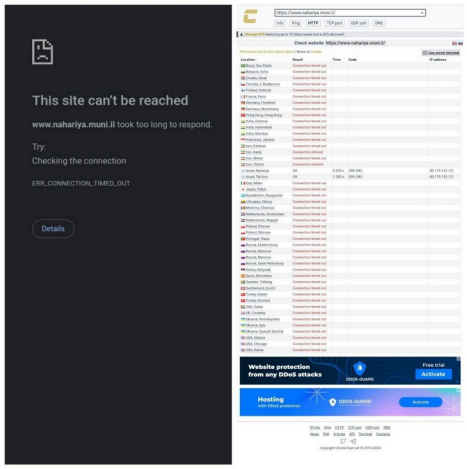
“Handala hacked soreq nuclear research center!
They got access to 197GB of the data of the center including emails, confidential maps, etc.”

Sunday, September 29, 2024

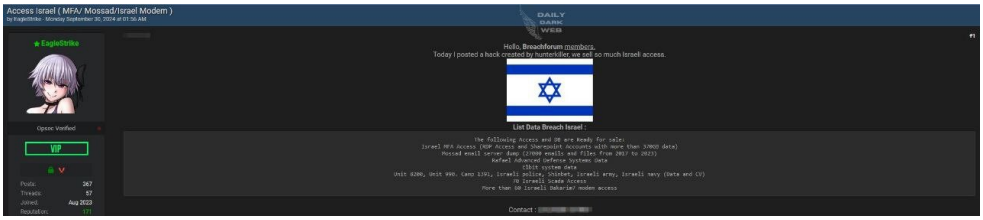

IDOR in AlrajhiBanks APIs
LONG TIME NO SEE EH ? DONT CONNECT THE DOTS PLEASE! IM NOT SAFE LULZZ
also theres bunch of other stuff can be useful for exploitation. Maybe a nosql? I'd idk maybe.
price: 695 BTC.
It needs fuzzing, or you need to know the targets cartID or any of the other bugs, needs a lil recon thats why its cheap.
I just happen to discover the issue.
Session if youre interested:
DAILY DARK WEB
VIP

“Vulnerability in KSA Bank!
IDOR Vulnerability in AI Rajhi Bank's APIs is for sale.”

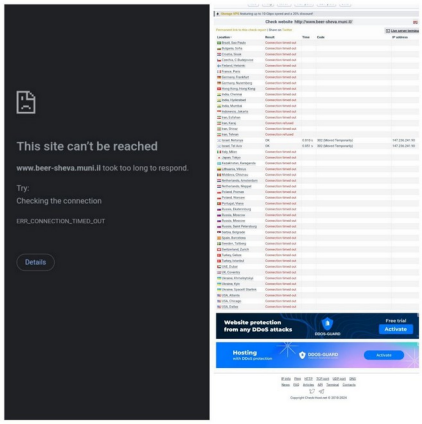
Monday, September 30, 2024



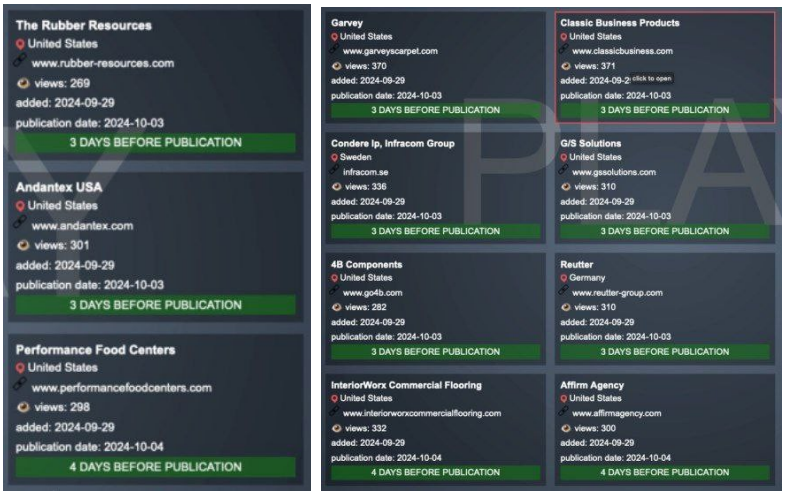
“**WebSec** took down Nahariya city official website!”


Access israel (MFA/ Mossad/Israel Modem)
EagleStrike
VIP
Hello, Breachforum members.
Today I posted a hack created by hunterkiller, we sell so much Israeli access.
List Data Breach Israel :
Contact :

“Data of High-profile institutions of Israel is for sale!”



“WebSec also attacked Beersheba official website!”



“USA, Sweden and Germany are new targets of PLAY ransomware group!”

Tuesday, 1 October 2024

“Well... I announce to you that we were able to gain access to the archives of www.sec.gov

Our team recently intercepted the US Securities and Exchange Commission. We have all the financial statements for 20 years of work. Yes, from 1994 to 2024 today.

Having leafed through these archives and looked through several reports, we discovered an interesting point. We will tell you now...

Are you familiar with JPMorgan Chase & Co ?
This is an American conglomerate, the largest transnational bank. Actually, on September 27, the www.sec.gov commission posted in its archives a report on the transfer of funds: the amounts there vary from $490,000 to $1.7 million. All transfers go to this bank, under the guise of subsidies. There are 35-40 such transfers per day. So, do you understand what amount of money the state structure allocates to this conglomerate, and even under the guise of subsidies?) And an equally interesting point is that Kiev cooperates with this conglomerate, and Zeleboba recently met with its representatives and signed papers on cooperation. Well, USA? Have you screwed up? Now you will be in a very unpromising position. Yesterday, when I took this data into work, I could not believe my eyes. But now I have put the whole picture together and outlined a scheme of how the money of US citizens flies to Ukraine. So that you understand, according to average

estimates, over 26 billion dollars have flown to Ukraine over the last year and a half using this scheme. This is the greatest disgrace for the Americans.

 Dear friends, I am attaching evidence straight from the archives of this interesting commission, sponsoring country 404. Glory to Russia!”

Thursday, October 3, 2024

“Handala attacked Haderi Haredim, the largest ultra-orthodox website in the world!
bhol.co.il
https://pikwy.com/web/66fdb7c5a87cd34052256459”

“UMC Health, provides health services in Texas, is under ransomware attack!”

Sunday, October 6, 2024

“Government websites and digital sevices of Wayne County in the USA are exposed to a cyberattack!”

Monday, October 7, 2024

“**USA data leak!**

2000 phone numbers of America and Canada has been leaked by UserSec!”

“Silver Shadow, one of the weapons production factories in Israel, is experiencing a cyberattack by Handala!
http://silver-shadow.com”

Wednesday, October 9, 2024

USA California Secretary of State + documents. 9gb
vadimblyaa
USA California Secretary of State + documents by me
download:
file password:
Breached
MEMBER
Information about the files inside:
debtors.csv
This file contains records of various organizations and individuals, likely debtors or entities associated with financial obligations
A unique identifier (e.g.,
A type (e.g., "Organization" or "Individual")
The entity's name (for organizations) or the individual's first, middle, last name
An address, including street, city, state, postal code, and country
The entities listed include businesses, pharmacies, service companies, and individuals, all of which are located in the United St
“Database of California secretary of state has been leaked!”

Thursday, October 10, 2024

“The largest water and wastewater Company in the US, American Company, has disabled parts of its computer systems due to a massive cyberattack!”

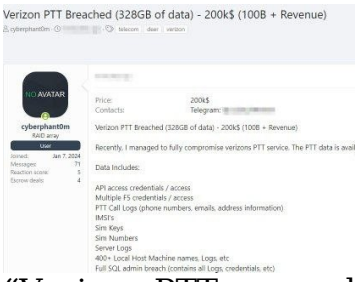
Friday, October 11, 2024

“1.3 million records of data of Lead Buyer, a US company specializing in the purchase of insurance and mortgage internet leads, has been leaked!”

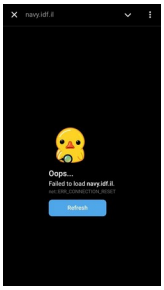
“Israeli Ministry of welfare is also under a dataleak!”

“Hunt3r kill3rs attacked IDF!
Over 200k records of data of IDF is in the hands of Hunt3r kill3rs!”

Saturday, October 12, 2024

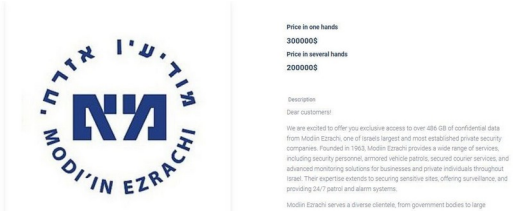

Verizon PTT Breached (328GB of data) - 200k$ (100B + Revenue)
cyberphant0m
RAID array
User
Price: 200k$
Contacts: Telegram:
Verizon PTT Breached (328GB of data) - 200k$ (100B + Revenue)
Recently, I managed to fully compromise verizons PTT service. The PTT data is avail
Data Includes:
API access credentials / access
Multiple F5 credentials / access
PTT Call Logs (phone numbers, emails, address information)
IMSI's
Sim Keys
Sim Numbers
Server Logs
400+ Local Host Machine names, Logs, etc
Full SQL admin breach (contains all Logs, credentials, etc)

“Verizon PTT, expands digital access, let 328GB of its data be in the hands of hackers!”

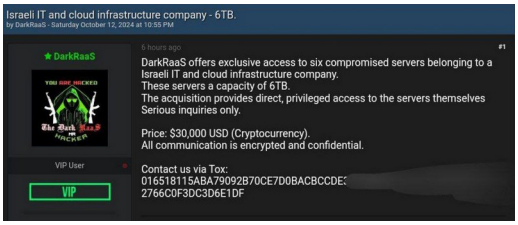


“Anonymous Collective attacked IDF navy website and it is currently out of service!”

Sunday, October 13, 2024



“Modiin Ezrachi is under a cyberattack and over 480GB of its data will be sold for $300k!”

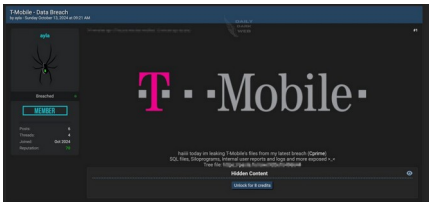

Israeli IT and cloud infrastructure company - 6TB.
by DarkRaaS - Saturday October 12, 2024 at 10:55 PM
DarkRaaS
6 hours ago
#1
DarkRaaS offers exclusive access to six compromised servers belonging to a Israeli IT and cloud infrastructure company.
These servers a capacity of 6TB.
The acquisition provides direct, privileged access to the servers themselves
Serious inquiries only.
Price: $30,000 USD (Cryptocurrency).
All communication is encrypted and confidential.
VIP User
VIP
Contact us via Tox:
016518115ABA79092B70CE7D0BACBCCDE
2766C0F3DC3D6E1DF

“Access to an IT company in Israel is for sale for $30k!”

“Also for sale, an access to cloud environment of a Municipality in Israel!”

Tuesday, October 15, 2024

“Cisco Breach!
An attacker sells internal information of Cisco.”



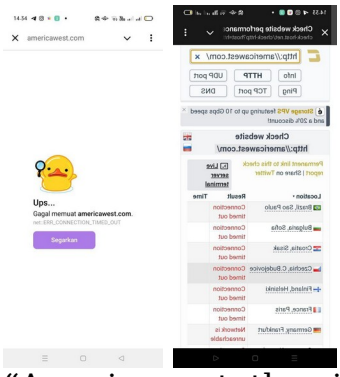
“**T-Mobile Data Breach!**
Critical files, including SQL database, internal programs, user reports, etc, have been leaked.”

Wednesday, October 16, 2024

“Evolution Mining, the Australian mining company, is under a ransomware attack!”

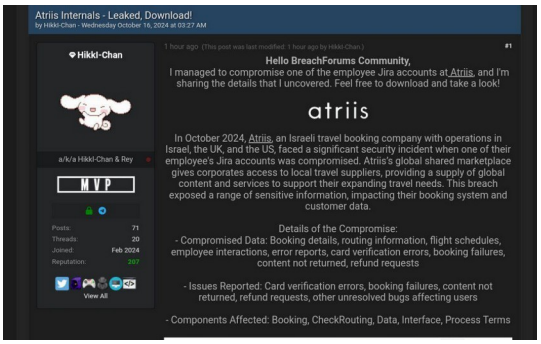
“Orion SA, a leading global supplier of carbon black, trapped into a fraud!”

“The Swiss company, Schlatter Group, suffers from a ransomware attack! Schlatter manufactures industrial machines.”

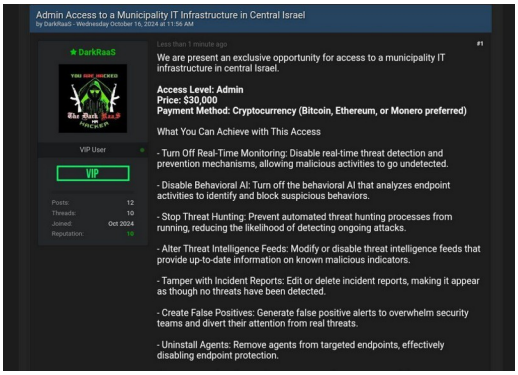


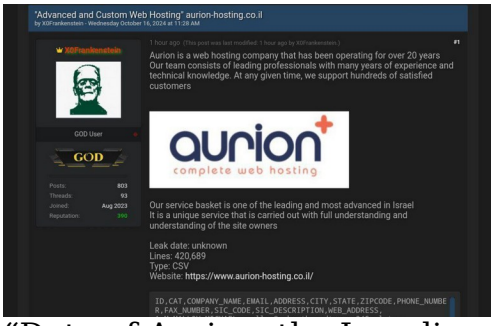
“Americawest, the airline company, has been hacked by DDOS TEAM ANONYMOUS!”

Thursday, October 17, 2024


Atriis Internals - Leaked, Download!
Hikki-Chan
Hello BreachForums Community,
I managed to compromise one of the employee Jira accounts at Atriis, and I'm sharing the details that I uncovered. Feel free to download and take a look!
atriis
In October 2024, Atriis, an Israeli travel booking company with operations in Israel, the UK, and the US, faced a significant security incident when one of their employee's Jira accounts was compromised. Atriis's global shared marketplace gives corporates access to local travel suppliers, providing a supply of global content and services to support their expanding travel needs. This breach exposed a range of sensitive information, impacting their booking system and customer data.
Details of the Compromise:
- Compromised Data: Booking details, routing information, flight schedules, employee interactions, error reports, card verification errors, booking failures, content not returned, refund requests
- Issues Reported: Card verification errors, booking failures, content not returned, refund requests, other unresolved bugs affecting users
- Components Affected: Booking, CheckRouting, Data, Interface, Process Terms
“Information of the Israeli company Atriis has been leaked!”

“**UK Bank!**
HSBC bank customers were scammed by fake SMS and the bank must compensate for them!”


Admin Access to a Municipality IT Infrastructure in Central Israel
DarkRaaS
We are present an exclusive opportunity for access to a municipality IT infrastructure in central Israel.
Access Level: Admin
Price: $30,000
Payment Method: Cryptocurrency (Bitcoin, Ethereum, or Monero preferred)
What You Can Achieve with This Access
- Turn Off Real-Time Monitoring: Disable real-time threat detection and prevention mechanisms, allowing malicious activities to go undetected.
- Disable Behavioral AI: Turn off the behavioral AI that analyzes endpoint activities to identify and block suspicious behaviors.
- Stop Threat Hunting: Prevent automated threat hunting processes from running, reducing the likelihood of detecting ongoing attacks.
- Alter Threat Intelligence Feeds: Modify or disable threat intelligence feeds that provide up-to-date information on known malicious indicators.
- Tamper with Incident Reports: Edit or delete incident reports, making it appear as though no threats have been detected.
- Create False Positives: Generate false positive alerts to overwhelm security teams and divert their attention from real threats.
- Uninstall Agents: Remove agents from targeted endpoints, effectively disabling endpoint protection.
“Pay $30,000 and get access to one of Municipalities IT infrastructure in Israel!”


"Advanced and Custom Web Hosting" aurion-hosting.co.il
Aurion is a web hosting company that has been operating for over 20 years
Our team consists of leading professionals with many years of experience and technical knowledge. At any given time, we support hundreds of satisfied customers
aurion
complete web hosting
Our service basket is one of the leading and most advanced in Israel
It is a unique service that is carried out with full understanding and understanding of the site owners
Leak date: unknown
Lines: 420,689
Type: CSV
Website: https://www.aurion-hosting.co.il/
“Data of Aurion, the Israeli company provides website management and hosting services, has been leaked recently!”

“Computer systems of Municipality of Calgary in Canada were shut down due to a massive cyberattack!”

On the discussion section of the channel, the following was posted by @PL4GU3_H4CKS with UID 1263317336:

“Need a hacker for hire!?
Look no further ! You’re now at a one stop shop .
Services include :

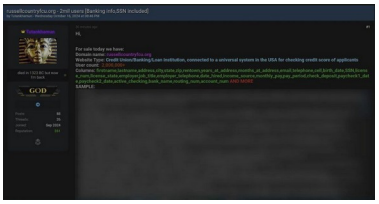
!!SQL Injection
!!Website Defacement
!!Spy on WhatsApp
!!Ddos attacks
!!Phishing Email
!!Hack Snapchat
!!Hack twitter
!!Cyber Espionage
!!Hack iCloud
!!Cross-Site Scripting(XXS)
!!Hacking/tracking mobile phone
!!Network Stiffing
!!Hack facebook
!!Hack instagram
!!DoS attacks
!!Crypto difficulties

‼Keylogging
‼Hack telegram
‼Hack Reddit
‼Bank Cheques
‼Crypto Jacking
‼Malware & Virus Deployment
‼Block lost ATM cards
‼Hack website
‼Hack University grade’s
‼Hack IP Cameras
‼Spark account activation.
‼Phishing script panel
‼Baiting
‼Instant chat trick
‼Cell Phone Monitoring
‼Tik Tok Hack
‼Spear Phishing
‼Lost Laptop Tracking
‼Tracking of lost vehicle
‼Change of Identity

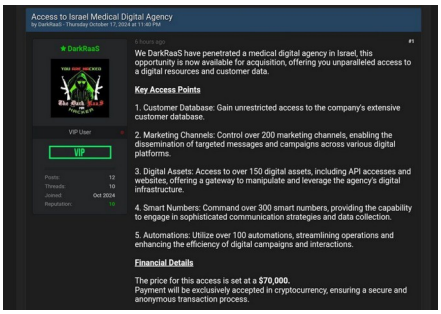
And lots more
Kindly send a message for more information.⁉

No free service ”

Friday, October 18, 2024



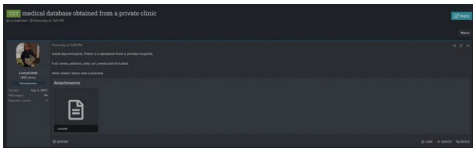
“Database of Russell Country Federal Credit Union (FCU) is for sale!”


Access to Israel Medical Digital Agency
DarkRaaS
VIP User
VIP
We DarkRaaS have penetrated a medical digital agency in Israel, this opportunity is now available for acquisition, offering you unparalleled access to a digital resources and customer data.
Key Access Points
1. Customer Database: Gain unrestricted access to the company's extensive customer database.
2. Marketing Channels: Control over 200 marketing channels, enabling the dissemination of targeted messages and campaigns across various digital platforms.
3. Digital Assets: Access to over 150 digital assets, including API accesses and websites, offering a gateway to manipulate and leverage the agency's digital infrastructure.
4. Smart Numbers: Command over 300 smart numbers, providing the capability to engage in sophisticated communication strategies and data collection.
5. Automations: Utilize over 100 automations, streamlining operations and enhancing the efficiency of digital campaigns and interactions.
Financial Details
The price for this access is set at a $70,000.
Payment will be exclusively accepted in cryptocurrency, ensuring a secure and anonymous transaction process.

“Israel medical digital agency is under a databreach!”

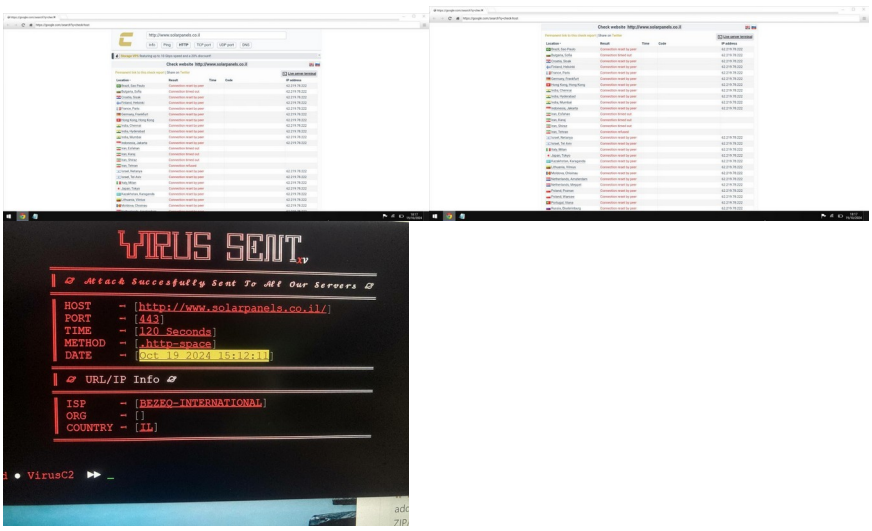
Royal Mail Data Breach - Leaked, Download!
Hello, BreachForums Community,
Today I have uploaded Royal Mail Data Breach for you to download, thanks for reading and enjoy!
Royal Mail
The Royal Mail Group Limited, trading as Royal Mail, is a British postal service and courier company.
In October 2024, Royal Mail suffered a small data breach which includes over 100 files with a total of 2,098 rows of data; however, I lost access relatively quickly and was therefore not able to exfiltrate all.
The breach did not occur directly through Royal Mail.
The Compromised Data Includes:
GOD
“And now UK!
Database of Royal Mail, the British postal service and courier company, has been leaked lately!”

itn.org.il - The Israel Tech Transfer Network (ITTN)
? Full Data Unveil: Israel Tech Transfer Network (ITTN)
'Unprecedented access to critical research data and personal details. No APT needed.'
Target: www.itn.org.il
Collected Data Includes:
DARK WEB
'Governments typically use APT to acquire this data. Here, it's available for free to everyone.'
About ITTN:
The Israel Tech Transfer Network (ITTN) is an organization that serves as a technology transfer network for leading Israeli universities and research institutions. It provides a bridge between academia and industry to promote innovation and research commercialization.
GOD
“Israel's Tech Transfer Network (ITTN) has been victim of a cyberattack!
Personal identifiable information (PII), research projects related to military, medicine and technology sectors were leaked.”



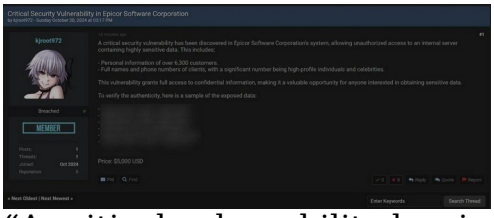
“Database of a clinic in USA has been leaked!”

Sunday, October 20, 2024

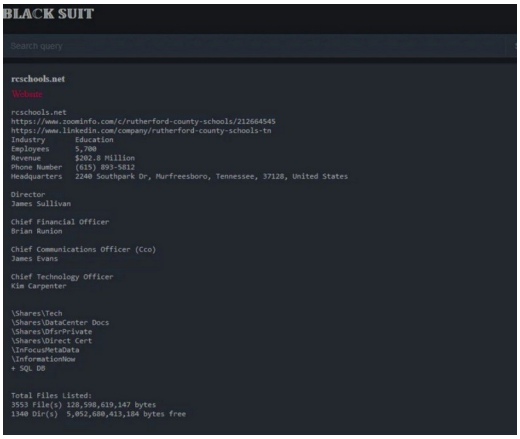


“Website of Renewable Energy Infrastructure of Israel has been hacked by Lulzsec Black!”

“Official website of Israel institute for foreign policy and national security studies was targeted by Mr.Hamza in collaboration with Moroccan Cyber Aliens!”



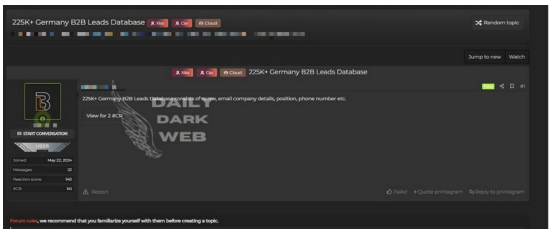
“A critical vulnerability has just been found in the American Epicor Server System!”



“The new victim of Black Suit Ransomware is Rutherford County Schools in the United States!”

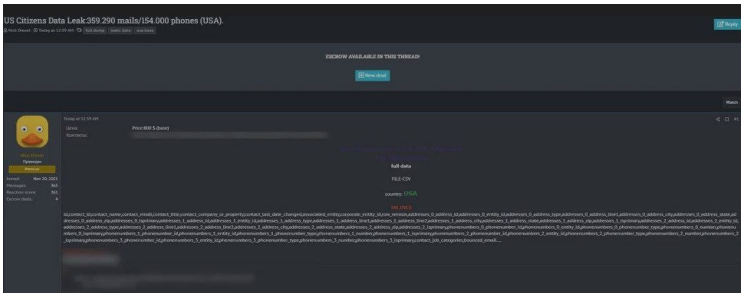
“**Stormous** ransomware group named it's latest victim, and it is Transak, a global web3 infrastructure services provider with registered entities in the USA, the UK and many more countries.”

Monday, October 21, 2024

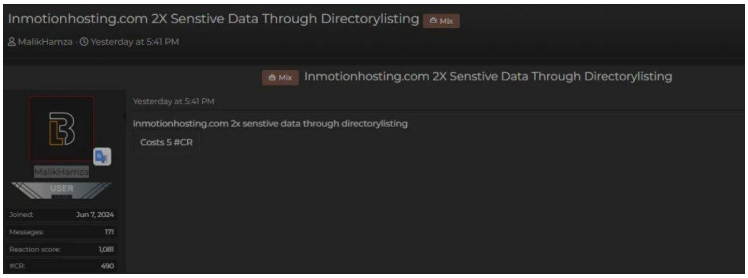


“Over 225k German B2B leads database were leaked!”

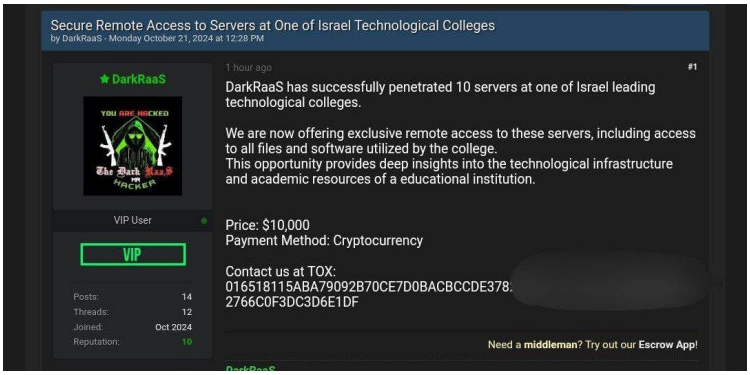
“Port of Haifa and the Israeli Ports company were hacked!
Workers received text messages from the attackers.”



“Data of US citizens have been leaked will be sold soon!”



“More from America!
This time data of inMotion Hosting has been leaked!”


Secure Remote Access to Servers at One of Israel Technological Colleges
by DarkRaaS - Monday October 21, 2024 at 12:28 PM
DarkRaaS
YOU ARE HACKED
VIP User
VIP
Posts: 14
Threads: 12
Joined: Oct 2024
Reputation: 10
1 hour ago
#1
DarkRaaS has successfully penetrated 10 servers at one of Israel leading technological colleges.
We are now offering exclusive remote access to these servers, including access to all files and software utilized by the college.
This opportunity provides deep insights into the technological infrastructure and academic resources of a educational institution.
Price: $10,000
Payment Method: Cryptocurrency
Contact us at TOX:
016518115ABA79092B70CE7D0BACBCCDE378.
2766C0F3DC3D6E1DF
Need a middleman? Try out our Escrow App!
“10 servers of a technological college in Israel are under massive cyberattack!
Access to the servers will be sold for $10k.”

On the discussion section, “Afro Samurai” with UID 8014642869 posted the following:

“The official Israel Defense Directory lists over 200 industries in nine categories: aerospace, naval forces, land forces, electronics,optronics, military inventory, HLS, Civil Defense and NBC protection
and services.
Source:
http://www.sibat.mod.gov.il/Industries/directory/Pages/default.aspx

www.aerosol.co.il

www.bsel.co.il
www.elbitsystem.com
www.iai.co.il
www.kanfit.com
www.aeromaoz.com

www.astronautics.co.il
www.bamicrowaves.co.il
www.epsilor.com

www.orbit-cs.com
www.pronatindustries.com
www.rafael.co.il
www.aerodan.com
www.mtcind.com
www.uvisionuav.com
www.birdaero.com
www.hartech.co.il
www.gilat.com
www.israel-shipyards.com
www.dsit.co.il
www.sibat.mod.gov.il
www.ashot.co.il
www.magam-safety.com
www.nimda.co.il
www.plasan.com
www.tamor.co.il
www.shladot.co
www.fibrotex-tech.com9
www.miframsecurity.com
www.hagor.com
www.lior-protective.com
www.myformgroup.com
www.rada.com
www.shalon.co.il
www.hosmd.com
www.ispraltd.com
www.cognyte.com
www.gmsecurity.com
www.cti-intl.co.il
www.yolandcorp.com
www.resheffuzes.com
www.cdntec.com
www.topcar-armoring.com
www.hba.co.il
www.karil.com
www.sansolo.co.il
www.epsilor.com

www.phantom-technologies.com
www.sk-g.net
www.nvisol.com
www.contact-kalia.com
www.emtan.co.il
www.mctdefense.com
www.rt.co.il
www.aeronautics-sys.com
www.bluebird-uav.com
www.spearuav.com
www.steadiccopter.com
www.smart-shooter.com
www.amstaf-ugv.com
www.imc-mw.com
www.magam-safety.com
www.nimda.co.il
www.plasan.com
www.tamor.co.il
www.shladot.com
www.fibrotex-tech.com
www.miframsecurity.com
www.hagor.com
www.lior-protective.com
www.maron-dolphin.com
www.myformgroup.com
www.rada.com
www.shalon.co.il
www.hosmd.com
www.ispraltd.com
www.cognyte.com
www.gmsecurity.com
www.cti-intl.co.il
www.yolandcorp.com
www.resheffuzes.com
www.cdntec.com
www.topcar-armoring.com
www.hba.co.il
www.karil.com
www.sansolo.co.il
www.epsilor.com
www.phantom-technologies.com
www.sk-g.net

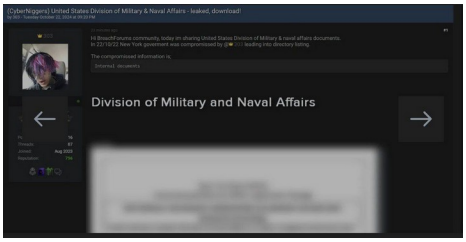
www.nvisol.com
www.contact-kalia.com
www.emtan.co.il
www.mctdefense.com
www.rt.co.il
www.aeronautics-sys.com
www.bluebird-uav.com
www.spearuav.com
www.steadiccopter.com
www.smart-shooter.com

www.amstaf-ugv.com
www.imc-mw.com
www.accubeat.com
www.commtact-systems.com
www.epsilor.com
www.gilat.net
www.mer-group.com
www.Orbit-cs.com
www.techaya.com
www.edgybees.com
www.prest.com
www.trilogical.com
www.tsgitsystems.com
www.cognyte.com
www.elta-ai.com
www.mipha.co.il
www.netlinetech.com
www.pic-six.com
www.waveguardtechnologies.com
www.controp.com
www.meprolight.com
www.optitask.net
www.troya-tech.com
www.uni-scope.co.il
www.ophiropt.com
www.opgal.com
www.scd.co.il
www.iard.co.il
www.ci-systems.com
www.laser-detect.com
www.cielo-inertial.com

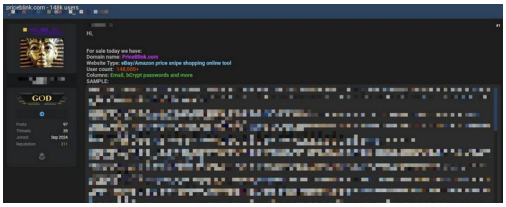
www.physical-logic.com
www.elmomc.com
www.tokagroup.com
www.rayzone.com
www.shalon.co.il
www.defensetechs.com
www.ludus-security.com
www.matrix.co.il
www.mlm-protection.com
www.morethansec.com
www.nirtal.com
www.bdo-shafran.co.il
www.iibr.gov.il
www.adcon.co.il
www.hoy2050.com
www.accubeat.com
www.commtact-systems.com
www.gilat.net
www.mer-group.com
www.techaya.com
www.edgebees.com
www.mprest.com
www.trilogical.com
www.tsgitsystems.com
www.elta-iai.com
www.mipha.co.il
www.netlinetech.com”

Wednesday, October 23, 2024

“VPN Access to several companies in USA is leaked!”



“Division of Military & Naval Affairs of USA suffers from a databreach!”



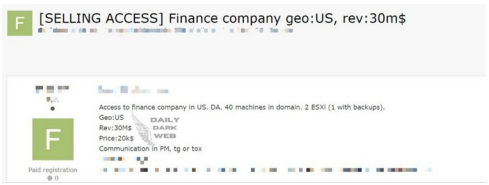
“Over 148k data of users of priceblink.com has been leaked”

“VideoToolBox is also another American company that is under a dataleak!”

“More than 1000 NHS accounts,UK, leaked!”

“107GB of data of Cordogan, Clark & Associates (CCA) has been leaked recently!
CCA is an architecture, planning and engineering firm based in Illinois with offices in Chicago, Aurora, Illinois, and Lafayette, Indiana.”

“Dataleak from 3 more American companies:
SendSMSNOW
Printavo
MatWeb LLC”



“Access to Finance Company Network of the US will be sold for $20k!”

Thursday, October 24, 2024

“After a short absence, Play Ransomware group showed up strongly!
Play Ransomware group announced six American companies as his new victims:

Ivanhoe Club
TU parks
Mainelli Mechanical Contractors
Action Heating
Eagle Heating
Iron World Manufacturing”

Saturday, October 26, 2024

“Hunt3r kill3rs published classified documents of Israel!
http://Campus.gov.il

“ElironNetworks attacked some Israeli websites and disabled all of them!
https://check-host.net/check-report/1f925af4k40e
https://check-host.net/check-report/1fa31ebck392
https://check-host.net/check-report/1fa37a12ke0b
https://check-host.net/check-report/1fa37995k2e7”

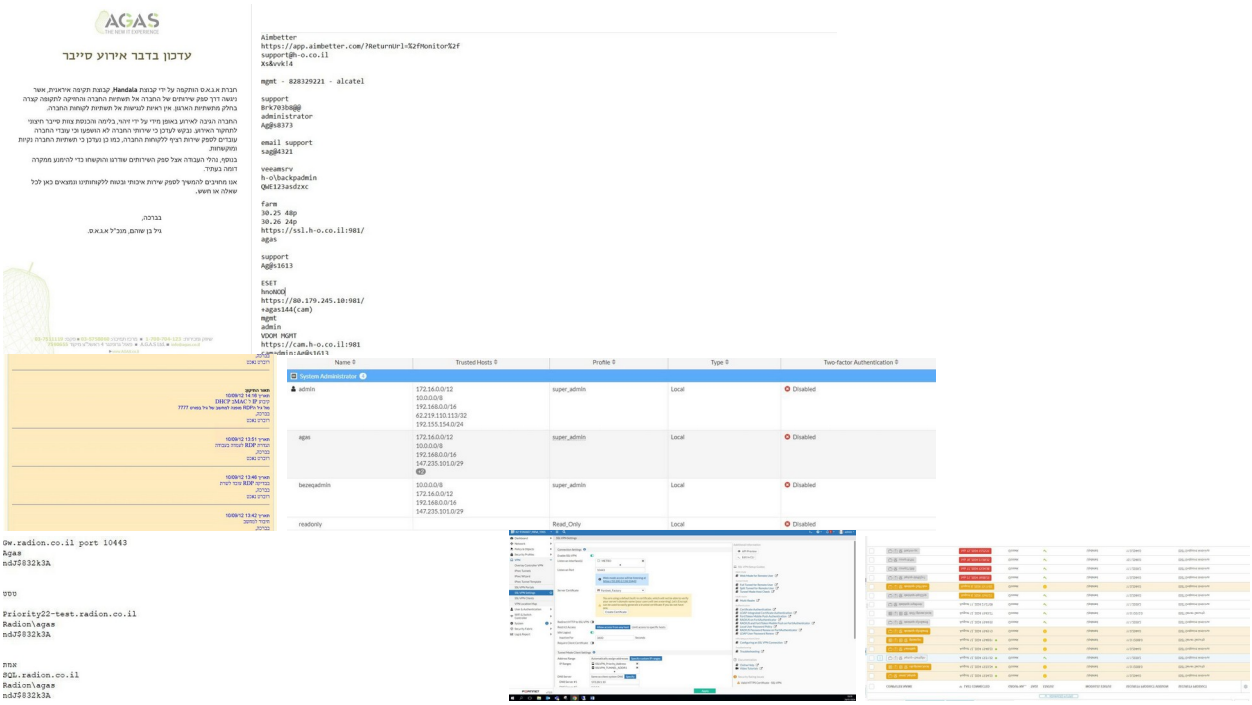
Sunday, October 27, 2024

“AGAS is the new target of Handala!
AGAS is a large company that provides cloud services & cyber security to 500 organizations.
Handala dumped 18TB of sensitive data from 74 servers.”

“Ransomhub announces an Israeli company as its new victim!
Payxpress provides financial solutions for pre-paid customers, such as cash payments for recurring bills (rent, electricity, and telephone), money transfers abroad, deposits to foreign bank accounts, and mobile wallet top-ups.”
http://payxpress.co.il”

“Several British website are out of service due to cyberattack by LulzSec Black!
https://colosseorestaurant.co.uk/wp-content/uploads/pls.html
https://holbeckrise.co.uk/wp-content/uploads/2024/10/IMG_20241023_191341_211.jpg
https://directory.cheddarchamber.co.uk/wp-content/uploads/2024/10/Hacked-By-LulzSec-Black.jpg
http://pro-feel.co.uk/wp-content/uploads/2024/10/pls-1.html
https://www.websearchseo.co.uk/wp-content/uploads/2024/10/IMG_20241023_191341_211-1.jpg”

Tuesday, October 29, 2024

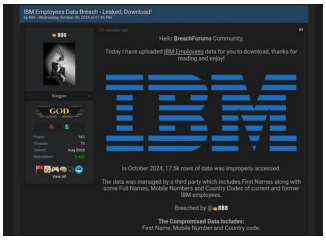


“Handala published 10GB of data of AGAS customers!”

“A big shame for IDF and Israel intelligence services!
Strava running app revealed data of Israeli soldiers along with accurate location of Hatzer & Tel Nof air force bases, the navy bases, the 8200 bases, the 504 intelligence unit, weapons depots (nuclear missiles storage), and US bases!”

“A cyberattack affected Free company!
43GB of data of the French company is for sale.”

Thursday, October 31, 2024


IBM Employees Data Breach - Leaked, Download!
Hello BreachForums Community,
Today I have uploaded IBM Employees data for you to download, thanks for reading and enjoy!
IBM
In October 2024, 17.5k rows of data was improperly accessed.
The data was managed by a third party which includes First Names along with some Full Names, Mobile Numbers and Country Codes of current and former IBM employees.
The Compromised Data Includes:
First Name, Mobile Number and Country code.
“Over 17k records of information of IBM has been leaked!”

“Hunt3r kill3rs got access to information of Israeli pilots and employees of Israel Air Force!”